IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Joachim Schmidt
Serial No.:	10/825,583
For:	PROCESS AND DEVICE FOR THE PACKET-ORIENTED TRANSMISSION OF SECURITY-RELEVANT DATA
Filed:	April 15, 2004
Examiner:	Christian A. LaForgia
Art Unit:	2439
Confirmation No.:	8182
Customer No.:	27,623

Attorney Docket No.: 2133.034USU

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

Dear Sir:

In response to the Office Action dated July 26, 2010, the period for response having been extended one month up to and including November 26, 2010, please amend the above-identified application as follows:

Listing of the Claims begins on page **2** of this paper.

Remarks begin on page **8** of this paper.

LISTING OF THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Previously presented) A process for the packet-oriented transmission of security-relevant data under application of at least one security-oriented message consisting of a first data packet and an allocated second data packet, and at least one transmission system with a parallel and/or serial network and/or bus system with at least one user connected to it, the process, comprising:

transmitting the security-relevant data and redundant information based on the security-relevant data within the at least one security-oriented message,

wherein, for each security-oriented message, the security-relevant data is transmitted in the first data packet and the redundant information, based solely on all the security-relevant data of the first data packet, is transmitted in the allocated second data packet of the at least one security-oriented message.

2. (Previously presented) The process according to claim 1, wherein the redundant information is encoded.

3. (Previously presented) The process according to claim 1, wherein the redundant information is a check sum (CRC) calculated over the security-relevant data.

4. (Previously presented) The process according to claim 1, wherein the security-relevant data is selected from the group consisting of user data, check data, and control data.

5. (Previously presented) The process according to claim 1, further comprising transmitting several packets within a predefined superset frame structure.

6. (Previously presented) The process according to claim 5, wherein the packets within a predefined superset frame structure include the security-relevant data and the redundant information that are allocated to each other.

7. (Previously presented) The process according to claim 1, wherein the packets with the security-relevant data and the redundant information that are allocated to each other are transmitted in a parallel or serial way.

8. (Previously presented) The process according to claim 1, wherein the packets with the security-relevant data and the redundant information that are allocated to each other are transmitted in strings or separately.

9. (Previously presented) The process according to claim 1, wherein the packets include an addressing block and/or an identification code for their logical allocation.

10. (Previously presented) A device for a transmission system with at least one parallel and/or serial network and/or bus system, for the packet-oriented transmission of security-relevant data under application of at least one security-oriented message consisting of a first data packet and an allocated second data packet, the device comprising:

means, arranged on the side of the sender, for the packet-oriented embedding of the security-relevant data into the first data packet and for the packet-oriented embedding of each allocated redundant information, based solely on all the security-relevant data of the first data packet, into the allocated second data packet of the security-oriented message.

11. (Previously presented) The device according to claim 10, further comprising an encoding device for the encoding of the redundant information.

12. (Previously presented) The device according to claim 10 wherein the means for embedding are allocated means for the generation of the redundant information with the same number of bits (n) as the security-relevant data to be transmitted.

13. (Previously presented) The device according to claim 10 wherein the means for the generation and/or embedding are designed such that any possible combination of the security-oriented data of a packet unambiguously results in exactly one of the possible combinations within the packet having the respective allocated redundant information.

14. (Previously presented) The device according to claim 10, further comprising means arranged on the side of the receiver for the verification of an error-free data transmission based on the security-relevant data embedded in at least one packet and the allocated redundant information, wherein each redundant information based on the security-relevant data of a respective one packet is embedded in a separate packet.

15. (Previously presented) The device according to claim 14 wherein the means for the verification are allocated means for reading out and allocating security-relevant data and allocated redundant information received in different packets.

16. (Previously presented) The device according to claim 10, wherein several packets with the security-relevant data and/or the allocated redundant information are capable of being transmitted within a predefined superset frame structure.

17. (Previously presented) The device according to claim 10, further comprising means for the packet-oriented embedding and readout of addressing blocks and/or identification codes for the logical allocation of individual packets and/or their contents to each other.

18. (Previously presented) The device according to claim 10, wherein the means are allocated to slave devices and/or a master device.

19. (Previously presented) A transmission system comprising:
at least one parallel and/or serial network and/or bus system; and
at least one device according to claim 10.

20. (Previously presented) The transmission system according to claim 19, wherein the network and/or bus system is at least one ring-, line-, star- and/or tree-shaped network and/or bus structure.

21-22. (Cancelled)

23. (Previously presented) The transmission system according to claim 19, wherein the at least one parallel and/or serial network and/or bus system comprises an Interbus system.

24. (Currently amended) A process for the packet-oriented transmission of security-relevant data under application of at least one transmission system with a parallel and/or serial network and/or bus system with at least one user connected to it, comprising:

forming at least one security-oriented message from two partial messages, the two partial messages including a first data packet and a second data packet;

transmitting the first data packet, via the at least one transmission system, the first data packet having only user data and check data, the first data packet totaling a first number of bits; and

transmitting the second data packet, via the at least one transmission system, the second data packet having only a check sum value calculated over the user data and the check data, the second data packet totaling a second number of bits that is equal to the first number of bits.

25. (Previously presented) The process according to claim 24, further comprising combining and jointly transmitting the first and second data packets within a frame structure.

26. (Previously presented) The process according to claim 24, further comprising transmitting the first and second data packets within different frame structures.

27. (Previously presented) The process according to claim 24, wherein the steps of transmitting the first and second data packets comprise separately transmitting the first and second data packets.

REMARKS

Claims 1-20 and 23-27 were presented for examination in the present application and remain pending upon entry of the instant amendment, which is respectfully requested. Claims 1, 10, and 24 are independent.

Rejection under 35 U.S.C. §101

Independent claim 24, as well as claims 25-27, were rejected under 35 U.S.C. §101 as being not patentable subject matter.

Applicant respectfully traverses these rejections.

Applicant submits that claims 24-27 do not fall within the three specific exceptions to §101's broad patent eligibility principles in that the pending claims are not directed to laws of nature, physical phenomena, or abstract ideas.

Clearly, independent claim 24 are **not** directed to laws of nature or physical phenomena. Also, and looking to the holding in *Gottschalk v. Benson*, 409 U.S. 63 (CCPA 1972), Applicant submits that independent claim 24 are **not** directed to abstract ideas.

Nonetheless, and merely in the interest of expediting prosecution, claim 24 has been amended to recite the steps of "transmitting the first data packet, via the at least one transmission system, the first data packet" and "transmitting the second data packet, via the at least one transmission system, the second data packet". This amendment merely makes explicit what had been implicit in the claim and clearly ties the method of claim 24 to the transmission system recited by the preamble.

Accordingly, reconsideration and withdrawal of the rejection under §101 to claim 24, as well as claims 25-27, are respectfully requested.

Rejection under 35 U.S.C. §102

Independent claims 1 and 10, as well as dependent claims 2-9 and 11-20, were rejected under 35 U.S.C. §102(e) over U.S. Publication No. 2003/0053454 to Katsavounidis et al. (Katsavounidis). Dependent claim 23 was rejected under 35 U.S.C. §103(a) over Katsavounidis in view of U.S. Publication No. 2003/0200323 to Dold et al. (Dold).

Applicant respectfully maintains the traversal of this rejection.

The Office Action asserts that Applicant previously argued features that were not recited by claim 1. Specifically, the Office Action asserts that Applicant previously argued that the "based solely on all the security-relevant data of the first data packet" element of claim 1 requires that for each packet containing user data, there is exactly one packet allocated that contains the respective redundant information.

Applicant respectfully disagrees. Applicant never argued, and are still not arguing, in the manner suggested by the Office Action.

Rather, claim 1 recites the step of "transmitting the security-relevant data and redundant information based on the security-relevant data within the at least one security-oriented message". Thus, the security-oriented message transmitted by claim 1 includes **within** that message both "**security-relevant data**" and "**redundant information**"

Further, claim 1 recites that "for **each** security-oriented message, the security-relevant data is transmitted **in the first data packet**" while the redundant information is "transmitted **in the allocated second data packet** of the at least one security-oriented message".

Thus, the first data packet has the security-relevant data, while the second data packet has the redundant information.

Importantly, claim 1 recites that the redundant information is "based **solely on all** the security-relevant data of the first data packet".

Stated another way, claim 1 requires that for **each** packet containing the security-relevant data (i.e., the first packet), there is a second packet that contains the redundant information, where this redundant information is based soley on all the security-relevant data of the first data packet. If the redundant information is based soley on all of the security-relevant data, then it is not based on anything but the security-relevant data.

In contrast, Katsavounidis discloses concatenating **selected portions of packet data corresponding to a plurality of frame packets** for a first frame; generating forward error correction bits for the concatenated selected portions of packet data; and transmitting the forward error correction bits in a separate packet identified with a user data identifier code or the like, including other unique identifier codes to be assigned in the future by MPEG-standards committee and the like. See paragraph [0017].

Thus, to the extent that "concatenated selected portions" of Katsavounidis can be read as the "redundant information" of claim 1, it is clear that Katsavounidis discloses that these concatenated selected portions correspond to a "**plurality of frame packets**" and, thus teaches away from the "redundant information" recited by claim 1 that is "**based solely on all the security-relevant data of the first data packet**".

Again, Katsavounidis discloses that each packet having FEC codes is for an amount of selected packets and hence there is not respectively one packet with FEC code allocated to each one packet with user data and further, there may also be packets with user data for which no FEC code is generated and allocated, such that there is no packet having redundant information that is based soley on all of the security-relevant information of another packet.

Accordingly, user data and redundancy data of claim 1 provide two packets of a security-oriented message that are arranged in a new and non-obvious way. Thus, the process of claim 1 does not require any additional data packets or redundancy information to be added.

In Katsavounidis, the FEC bits represent additional redundancy information, which is placed in the same packet as the user data or in an additional packet after the regular frame or VOP to ensure MPEG compatibility. Thus, as the FEC bits are added to video data stream to enhance its error resiliency, data length is increased.

In fact, the Office Action itself acknowledges that claim language specifying that the second packet only contains redundant information pertaining to the first data packet distinguishes over Katsavounidis. Instead, the Office Action asserts that Applicant's Admitted Prior Art (AAPA) of Figure 3 discloses this element.

First, Applicant submits that even if such an assertion was true, claim 1 was not rejected in view of the AAPA.

Additionally, Applicant submits that Figure 3 also does not disclose or suggest "redundant information" as recited by claim 1 that is "**based solely on all** the security-relevant data of the first data packet".

Figure 3 illustrates that the first and second packets are identical, namely both include the user data, the check data, and the CRC. In contrast, claim 1 does not require the first and second packets to be identical. Rather, claim 1 requires that the "redundant information" as recited by claim 1 that is "**based solely on all** the security-relevant data of the first data packet".

Accordingly, Applicant respectfully submits that claim 1, as well as claims 2-9 that depend therefrom, are in condition for allowance. Reconsideration and withdrawal of the rejection to claims 1-9 are respectfully requested.

Independent claim 10 now recites "means, arranged on the side of the sender, for the packet-oriented embedding of the security-relevant data into the first data packet and for the packet-oriented embedding of each **allocated redundant information, based solely on all the security-relevant data of the first data packet**, into the allocated second data packet of the security-oriented message (emphasis added)".

As discussed in detail above, Katsavounidis merely discloses concatenating **selected portions of packet data corresponding to a plurality of frame packets** for a first frame. See paragraph [0017]. As such, and to the extent that "concatenated selected portions" of Katsavounidis can be read as the "allocated redundant information" of claim 10, it is clear that Katsavounidis discloses that these concatenated selected portions correspond to a "**plurality of frame packets**" and, thus teaches away from the "allocated redundant information" recited by claim 10 that is "**based solely on all the security-relevant data of the first data packet**".

Thus, claim 10 also requires that the redundant information is based soley on all of the security-relevant information, whereas Katsavounidis discloses that each packet

having FEC codes is for an amount of selected packets and hence there is not respectively one packet with FEC code allocated to each one packet with user data.

Additionally, user data and redundancy data of claim 10 provide two packets of a security-oriented message that are arranged in a new and non-obvious way that do not require any additional data or redundancy information to be added, which is not disclosed or suggested by the additional FEC bits added by Katsavounidis.

The Office Action fails to assert that Dold to cure the aforementioned deficiencies of Katsavounidis.

Accordingly, Applicant respectfully submits that claim 10, as well as claims 11-20 that depend therefrom, are in condition for allowance over the cited art alone or in combination. Reconsideration and withdrawal of the rejection to claims 11-20 are respectfully requested.

Rejection under 35 U.S.C. §103

Independent claim 24, as well as dependent claims 25-27, were rejected under 35 U.S.C. §103(a) over Applicant's Admitted Prior Art in view of Katsavounidis.

Applicant respectfully traverse this rejection.

However, in the interest of expediting prosecution, claim 24 has been clarified to recite that the first data packet has "only user data and check data", while the second data packet has "only a check sum value calculated over the user data and the check data". Emphasis added.

Applicant respectfully submits that the cited art fails to disclose or suggest the step of "forming at least one security-oriented message from two partial messages" in

the manner recited by clarified claim 24. Thus, claim 24, as well as claims 25-27 that depend therefrom, are patentable over the cited art.

Conclusion

In view of the above, it is respectfully submitted that the present application is in condition for allowance. Such action is solicited.

In the alternative, Applicant submits that the instant amendment places the present application in better condition for appeal. Further, the instant amendment merely amends claim 24 to make explicit what had been implicit in the claims. Thus, Applicant submits that the instant amendment does not require further search and consideration. Accordingly, entry and consideration of the instant amendment, at least for the purposes of appeal, are respectfully requested.

If for any reason the Examiner feels that consultation with Applicant's attorney would be helpful in the advancement of the prosecution, the Examiner is invited to call the telephone number below.

Respectfully submitted,

October 27, 2010

/Edward L. McMahon/
Edward L. McMahon
Reg. No. 44,927
Attorney for Applicant(s)
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
One Landmark Square, 10th floor
Stamford, CT 06901-2682
Tel: (203) 327-4500
Fax: (203) 327-6401